



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/711,413	09/17/2004	Yung-Cheng Shih	FTCP0037USA	5412

27765	7590	10/22/2007
NORTH AMERICA INTELLECTUAL PROPERTY CORPORATION		
P.O. BOX 506		
MERRIFIELD, VA 22116		

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

NOTIFICATION DATE	DELIVERY MODE
10/22/2007	ELECTRONIC

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

winstonhsu.uspto@gmail.com  
Patent.admin.uspto.Rcv@naipo.com  
mis.ap.uspto@naipo.com.tw

3

<b>Office Action Summary</b>	<b>Application No.</b> 10/711,413	<b>Applicant(s)</b> SHIH, YUNG-CHENG	
	<b>Examiner</b> Longbit Chai	<b>Art Unit</b> 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 17 September 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-54 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-54 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 17 September 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2131

## DETAILED ACTION

### *Priority*

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 9/17/2004 but has a foreign priority application filed on 4/19/2004.

### ***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1, 3, 4, 7, 9, 10, 13, 15 – 18, 20, 21, 23, 25, 27 – 29, 33, 37, 41, 43 – 46, 50 and 52 – 54 are rejected under 35 U.S.C. 102(b) as being anticipated by Unger et al. (U.S. Patent 2003/0026423).

As per claim 1, Unger teaches a method for accessing discrete data comprising:

(a) transmitting a write command to a memory (Unger: Para [0064]);

(b) according to a data format of a file that is to be written into the memory,

determining whether each data following a header of the file needs to be encrypted, and transmitting the file header and each data following the file header to a logic unit (Unger: Para [0081], Para [0064] and Para [0089] & Figure 6 / Figure 7: (a) the data stream and corresponding data packets are considered to be conformed to a data format of a file (b)

Art Unit: 2131

the PID (packet identifier) determines whether the packet should be encrypted or not and (c) Figure 7 (& Figure 6 / Element 316) indicates the selection logic that needs to either turn-on the encrypting function or turn-off the encrypting function to directly inserting the clear packet into the output stream);

(c) turning on the logic unit for encrypting the data determined to be encrypted in step (b) and writing the encrypted data into the memory (Unger: see above (a) & Para [0058] / Para [0127]);

(d) turning off the logic unit for writing the data determined not to be encrypted in step (b) into the memory directly (Unger: see above (a) & Para [0058] / Para [0065] / Line 20 – 21); and

(e) sending a first response signal from the memory when the writing of the file is finished (Unger: Para [0127] / [0141]: the use of primary and secondary flags can be replaced with a counter matching test function to assure the integrity of the data stream – This can be considered as a response signal from the memory when the writing of the file is finished for data integrity assurance).

As per claim 7, 18, 33 and 37, the claim limitation is similar to claim 1 except the only difference of decrypting versus encrypting and read function versus the write function where the encryption / decryption and write / read functions are considered as a-MUST of a pair of system functions. Therefore, see same rationale addressed above in rejecting claim 1.

As per claim 29, Unger teaches a discrete data accessing system comprising:  
a memory for storing data (Unger: Para [0064]);

Art Unit: 2131

a first logic unit electrically connected to the memory for encrypting input data according to a predetermined encryption algorithm, writing the encrypted data into the memory, or writing input data into the memory directly (Unger: Para [0081], Para [0064] and Para [0089] & Figure 6 / Figure 7: (a) the data stream and corresponding data packets are considered to be conformed to a data format of a file (b) the PID (packet identifier) determines whether the packet should be encrypted or not and (c) Figure 7 (& Figure 6 / Element 316) indicates the selection logic that needs to either turn-on the encrypting function or turn-off the encrypting function to directly inserting the clear packet into the output stream); and

a second logic unit electrically connected to the first logic unit for determining whether each data following a header of a file that is to be written into the memory needs to be encrypted according to a data format of the file in order to decide whether to turn on the first logic unit for encrypting the input data and writing the encrypted data into the memory, or to turn off the first logic unit for writing the input data into the memory directly (Unger: see above (a) & Para [0058] / Para [0065] / Line 20 – 21).

As per claim 46, the claim limitation is similar to claim 1 except the only difference of decrypting versus encrypting and read function versus the write function where the encryption / decryption and write / read functions are considered as a-MUST of a pair of system functions. Therefore, see same rationale addressed above in rejecting claim 29.

As per claim 3, 9 and 20, Unger teaches the first response signal is a writing succeeded signal (Unger: Para [0127] / [0141]: the use of primary and secondary flags can be replaced with a counter matching test function to assure the integrity of the data

Art Unit: 2131

stream – This can be considered as a response signal from the memory when the writing of the file is finished for data integrity assurance).

As per claim 4, 10 and 21, Unger teaches transmitting the file header and each data following the file header from a plurality of buffers in turn to the logic unit in step (b) (Unger: Para [0127] Para [0129]: the SD RAM are allocated with a plurality of buffers / blocks having a pre-determined cache buffer size).

As per claim 13, 23, 41 and 50, Unger teaches the memory is a flash memory (Unger: Para [0151]).

As per claim 15, 25, 43 and 52, Unger teaches the memory is a digital video disk (DVD) (Unger: Para [0147]).

As per claim 16, 27, 44 and 53, Unger teaches the file is an audio file (Unger: Page 4 / Para [0042]).

As per claim 17, 28, 45 and 54, Unger teaches the file is a video file (Unger: Page 4 / Para [0042]).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject

Art Unit: 2131

matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 2, 8, 19, 30, 34, 38 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Unger et al. (U.S. Patent 2003/0026423), in view of Pinder et al. (U.S. Patent 5,684,876).

As per claim 2, Unger does not teach the data following the file header comprises one or a plurality of frames, in which each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be encrypted, and the data block of each frame is determined to be encrypted in step (b).

However, Pinder teaches the data following the file header comprises one or a plurality of frames, in which each frame comprises a header, a data block and a residual block, wherein the remainder of the difference between the number of bytes of a frame and the number of bytes of the frame header divided by 8 is a first number, and the residual block is the set of the last first number bytes of the frame, wherein the header and the residual block of each frame are determined not to be encrypted, and the data block of each frame is determined to be encrypted in step (b) (Pinder: Column 3 Line 32 – 33 / Line 51 – 65: (a) DES encryption has a block size of 8 bytes (b) encryption is performed on payload data only (header data is unencrypted) and (c) for a payload of less than 8 bytes (e.g. residual block) is also preferably not encrypted).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Pinder within the system of Unger

Art Unit: 2131

because (a) Unger teaches providing partial encryption and decryption of digital of television signals including video, audio and data and multiplexing a plurality of multimedia data stream packets (Unger: Para [004] and Figure 6 / 7) and (b) Pinder teaches encrypting multiplex data stream transport packets under MPEG 2 (Motion Picture Experts Group version 2) standards, and more specifically to a technique for encrypting an MPEG 2 payload where the size of the payload may not be necessarily be an integer multiple of a DES encryption algorithm block size (Pinder: Column 1 Line 10 – 15).

As per claim 8, 19, 30, 34, 38 and 47, the claim limitation is similar to claim 1 except the only difference of decrypting versus encrypting and read function versus the write function where the encryption / decryption and write / read functions are considered as a-MUST of a pair of system functions. Therefore, see same rationale addressed above in rejecting claim 2.

4. Claims 5, 11, 22, 31, 35, 39 and 48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Unger et al. (U.S. Patent 2003/0026423), in view of Rose et al. (U.S. Patent 2004/0071289).

As per claim 5, 11, 22, 31, 35, 39 and 48, Unger does not teach changing the data format from little-endian to big-endian, or changing the data format from big-endian to little-endian before writing the encrypted data into the memory.

However, Rose teaches changing the data format from little-endian to big-endian, or changing the data format from big-endian to little-endian before writing the encrypted data into the memory (Rose: Para [0083] Line 8 – 17: a translation between different

Art Unit: 2131

machine formats of little-endian and big-endian is required for an efficient stream ciphering).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rose within the system of Unger because (a) Unger teaches providing partial encryption and decryption of digital of television signals using a plurality of encryption algorithms (Unger: Para [004] and Figure 6 / 7) and (b) Rose teaches an efficient stream ciphering that includes a translation between different machine formats of little-endian and big-endian as needed (Rose: Para [0083] Line 1 – 2/ Line 8 – 17).

5. Claims 6, 12, 14, 24, 26, 32, 36, 40, 42, 49 and 51 are rejected under 35 U.S.C. 103(a) as being unpatentable over Unger et al. (U.S. Patent 2003/0026423), in view of Qawami et al. (U.S. Patent 7,227,952).

As per claim 6, 12, 26, 32, 36, 40 and 49, Unger does not teach the encryption (or decryption) algorithm is performed according to the specification of content protection for recordable media (CPRM).

However, Qawami teaches the encryption (or decryption) algorithm is performed according to the specification of content protection for recordable media (CPRM) (Qawami: Column 11 Line 16 – 17 / Line 29 – 31).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rose within the system of Unger because (a) Unger teaches providing partial encryption and decryption of digital of television signals using a plurality of encryption algorithms (Unger: Para [004] and Figure 6 / 7) and (b) Qawami teaches to secure playback of digital audio, video of multimedia

Art Unit: 2131

content from memory cards, compacts disks or other media by using media key block and a standard encryption / decryption algorithm of Content protection for recordable Media (CPRM), where the data block / chunk number is used as the index to the Media Key Block of a selected chunk data and the row and column are used to map to where the encrypted media keys are stored for data protections (Qawami: Column 2 Line 9 – 10 and Column 11 Line 16 – 17 / Line 29 – 31).

As per claim 14, 24, 42 and 51, Unger as modified teaches the memory is a secure digital (SD) card (Qawami: Column 2 Line 33 – 35).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Rose within the system of Unger because (a) Unger teaches providing partial encryption and decryption of digital of television signals using a plurality of encryption algorithms (Unger: Para [004] and Figure 6 / 7) for a secure content delivery system such as DirecTV, DSS (Digital Satellite Service) as well as package media (e.g. CD and DVD, etc.) (Unger: Para [0147]) and (b) Qawami teaches to secure playback of digital audio, video of multimedia content from memory cards and a package media (e.g. CD, DVD and secure digital (SD) card) by using a standard encryption / decryption algorithm of Content protection for recordable Media (CPRM) (Qawami: Column 2 Line 9 – 10 / Line 33 – 35, Column 11 Line 16 – 17 / Line 29 – 31).

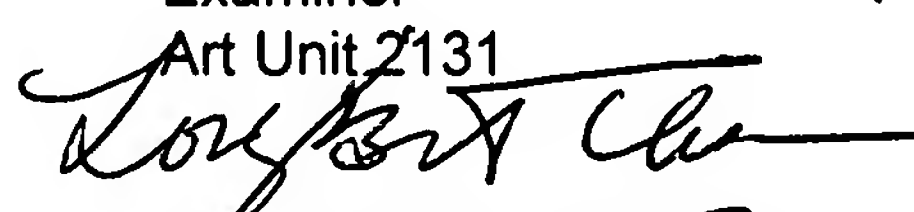
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

  
LBC

Longbit Chai  
Examiner  
Art Unit 2131  
  
10/2/2007